BEACON HR/PAYROLL IMPLEMENTATION PROJECT
SAP SECURITY STRATEGY

TABLE OF CONTENTS

1. INTRODUCTION 1
2. SECURITY METHODOLOGY 2
3. PRODUCTION SECURITY DESIGN APPROACH 3
3.1. SAP Application Security Construct 3
3.2. Transaction to Role Mapping 5
3.3. Role to Position Mapping 6
4. SAP SECURITY ORGANIZATION HIERARCHY 6
4.1. SAP Security Organization Hierarchy Requirements 7
4.2. Common Organizational Areas for Securing SAP Hierarchies 7
4.3. Using SAP Derived Roles for SAP Security Organization Hierarchy 8
5. TECHNICAL SECURITY GUIDELINES 9
5.1. Program and Report Security 9
5.2. Table Security 9
5.3. Spool Security 10
5.4. Printer Security 10
5.5. Default SAP User IDs 11
5.6. Client 000, 001, 066 11
5.7. SAP_ALL 12
6. USER MENU 12
7. USER ID 12
7.1. User ID Naming Convention 12
7.2. User ID Automation Strategy 13
7.3. Deactivating User IDs in SAP 13
7.4. Transferred or Terminated Employee Process 13
8. CENTRAL USER ADMINISTRATION 14
9. PASSWORD ADMINISTRATION 14
10. SAP SYSTEM SETTINGS 15
11. SINGLE SIGN-ON 16
12. SEGREGATION OF DUTIES STRATEGY 16
13. SAP USER GROUPS 17
14. SECURITY AUDIT LOGGING AND REPORTING 17

15. CHANGE CONTROL FOR SECURITY 17
16. SAP ENVIRONMENTS 18
16.1. Sandbox Systems 18
16.2. Development Systems – ERP2005 Configuration Client 18
16.3. Development Systems – ERP2005 ABAP development Client 18
16.4. Development Systems – ERP2005 Security Client 18
16.5. Development Systems – Business Intelligence (BI) 19
16.6. Quality Assurance and Testing Systems - Integration Testing Client 19
16.7. Training Client(s) 19
16.8. Production Systems 19
17. SENSITIVE DATA 19
18. SECURITY TESTING 20
19. SAP SECURITY REQUEST PROCESS 20
19.1. Production 20
19.2. Sandbox/Development/QAS 20
20. SECURITY ROLE NAMING CONVENTION 21
20.1. SAP ERP2005, BI, Solution Manager 21
20.1.1. Sandbox/Development/QAS 22
20.1.2. Production 23
20.2. SAP Portal 24
20.2.1. Portal Roles 24
20.2.2. Portal Groups 24
APPENDIX A: SAP SECURITY TERMINOLOGY OVERVIEW 25
APPENDIX B: SAP SANDBOX/DEV/QAS USER REQUEST FORM 27

1. INTRODUCTION

The State of NC is implementing SAP under the project known as "Beacon". The first phase being implemented under Beacon is SAP HR Module. The Beacon project consists of ERP 2005 - HR Organizational Management, Personnel Administration, Benefits Administration, Time Management, Payroll Administration, Training and Events, along with ESS/MSS via the SAP Portal. Also, SAP's Business Warehousing System (BI – Business Intelligence) is being implemented to achieve additional reporting requirements.

Additionally, to support the HR module, pieces of Finance (FI), Controlling (CO) and Funds Management (FM) master data will be loaded into SAP. Full Implementation of FI, CO, and FM will be part of another phase.

The functionality offered in SAP ERP2005 (R/3) and BI is allowing the State of NC to replace several different legacy systems. The implementation of ERP software increases functionality as well as process integration, while at the same time, increasing potential vulnerability. Actions that currently are performed on several different systems in different locations provided security control. Since all agencies will now be sharing one system, the need to implement proper security is critical.

SAP Application Security is a key component of the overall implementation of the SAP application. To enable an effective and efficient design and implementation of SAP application security, we have established an architecture that will form a common framework for the Beacon project. This document contains the elements of the approach to SAP Security, including:

- SAP Security Thread of ProvenCourse Methodology
- Production Security Design Approach
- SAP Security Organization Hierarchy Principles
- Technical Security Guidelines
- Security Naming Conventions
- SAP System Settings
- SAP Security Access Request Process

This SAP Security Strategy document should be referenced when designing, implementing and maintaining SAP application security. This document describes the approach for the development of SAP Application Security. SAP Security Policies and Procedures for the production environment will be developed during the last phase of the project. The SAP Security Policies and Procedures include detailed information on how to maintain the security of the Beacon SAP environments.

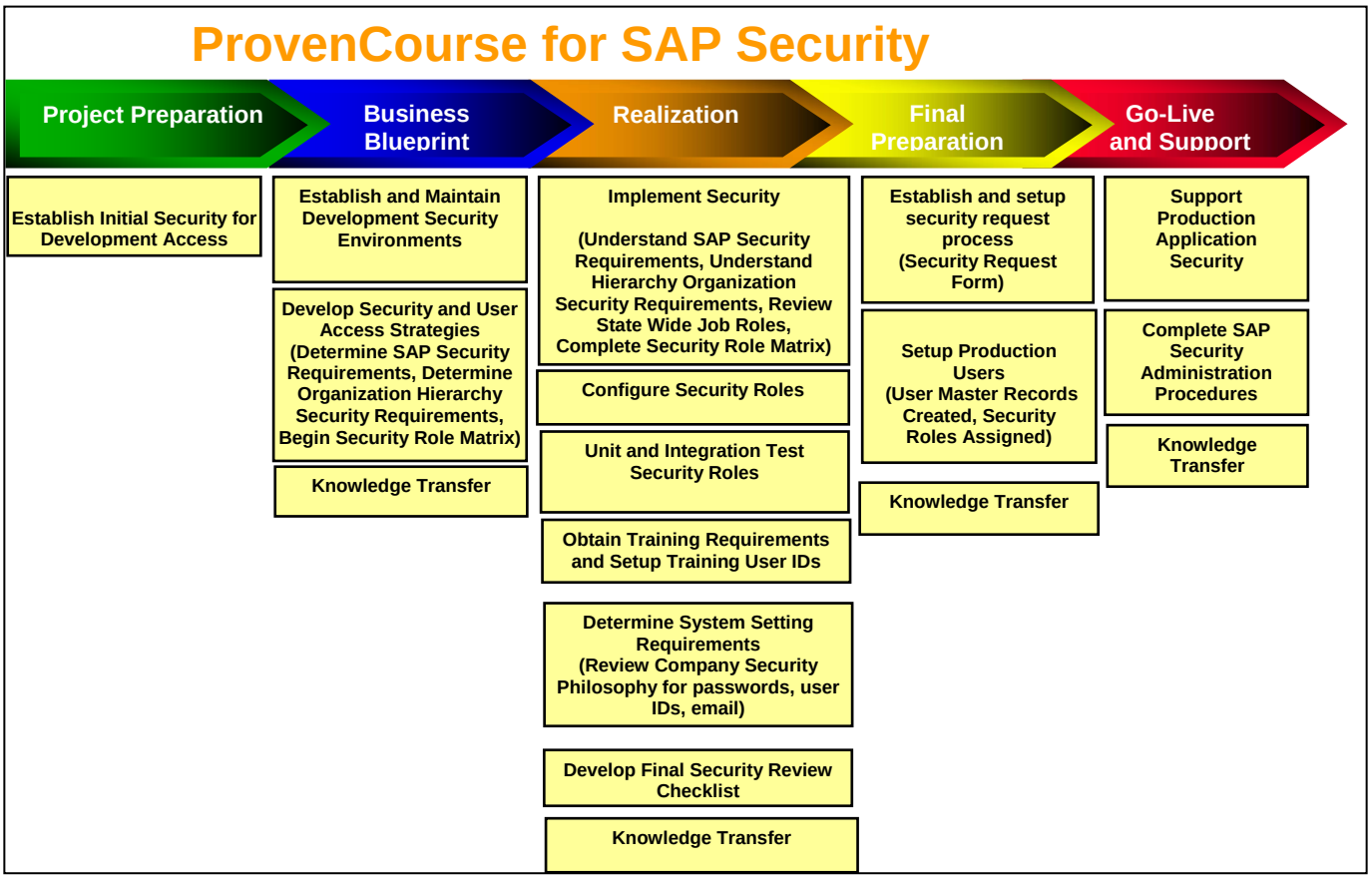
2. SECURITY METHODOLOGY

Security has a thread within the ProvenCourse Methodology. The ProvenCourse Methodology is based on a 'Roadmap' concept. The Roadmap acts as a guide for the project, specifying steps, identifying milestones, and setting the pace for the entire project.

The Roadmap consists of five phases:

- Phase 1: Project Preparation (initial scoping/planning)
- Phase 2: Business Blueprint (data gathering)
- Phase 3: Realization (configuration and testing)
- Phase 4: Final Preparation (training and cut-over)
- Phase 5: Go-live and Support (actual go-live)

ProvenCourse for SAP Security include designing, configuring and testing the security roles for go-live. The next sections of this document describe how production security will be designed and tested.



3. PRODUCTION SECURITY DESIGN APPROACH

The access controls designed for the production environment are closely aligned to the business processes that are established by the functional teams. These controls facilitate and do not hamper the business functions, while maintaining compliance with the State of NC policies.

The extent of access controls are being designed with the proper level of authority and restrictions while taking into consideration other controls that are in place. Other compensating controls such as monitoring and reconciliation will be used to mitigate some risks.

The access controls designed are flexible and maintainable. The design leads to efficiency in on-going security maintenance and administration. The design allows for an efficient means to add new agencies or re-organize agencies.

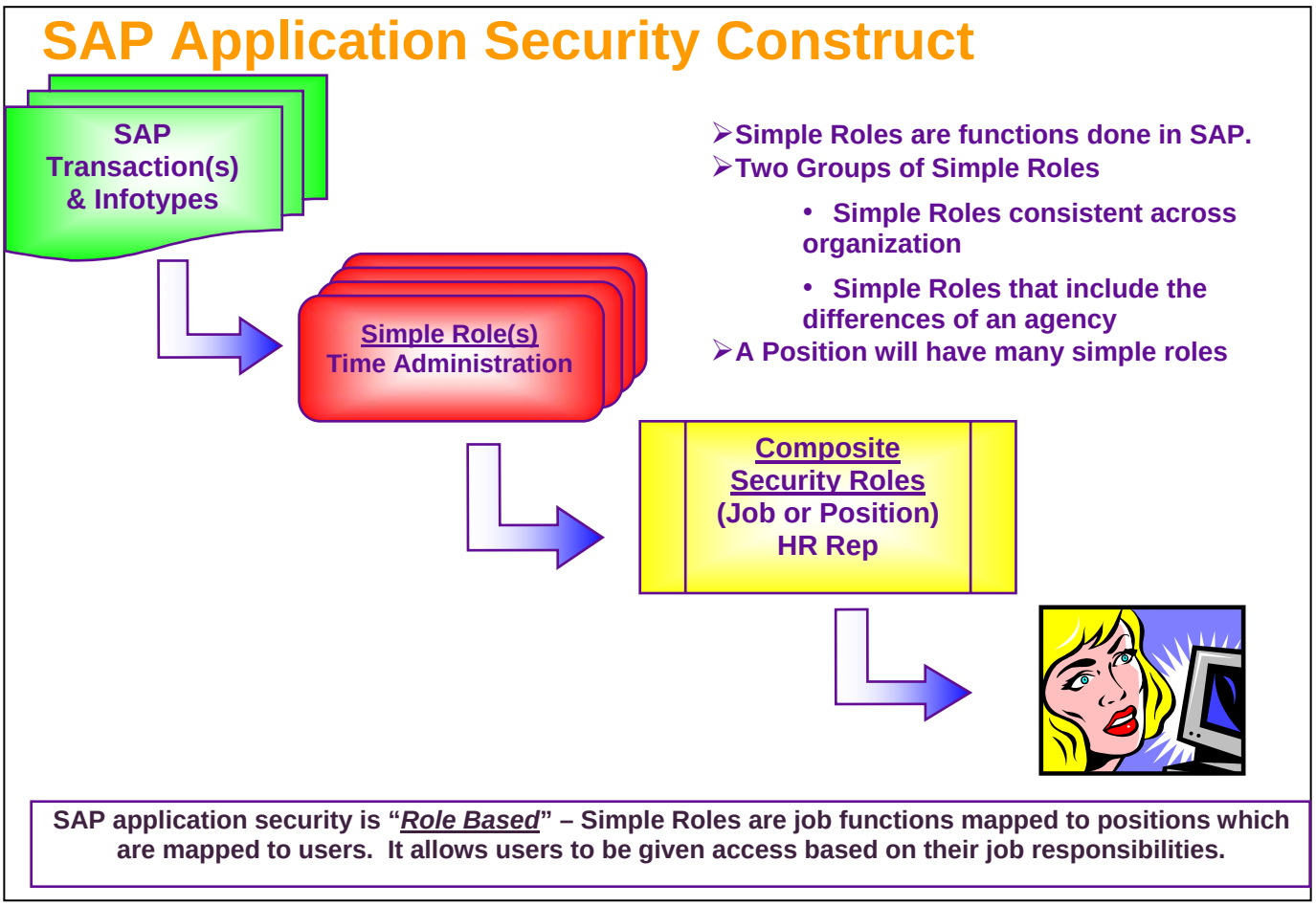
The SAP Profile Generator will be the primary tool in building and maintaining security. Profile Generator is a tool provided by SAP and resides within the SAP application. It is used to create and maintain security roles. SAP has a guide called "Authorizations Made Easy" that shows step-by-step instructions on how to use the Profile Generator tool. Authorizations Made Easy manual will be referenced in the SAP Security Policies and Procedures to reduce redundancies in explaining how to use the tool since SAP has already documented the tool extensively.

3.1. SAP Application Security Construct

The SAP Authorization Concept will be used to secure access to the application functions. The Security Construct follows the SAP Authorization Concept. SAP Authorization Concept is "Role Based". Roles are job functions mapped to positions which are mapped to users. It allows users to be given access based on their job responsibilities. To design end user security for the production environment, the SAP Security Team starts with identifying what functions, including transaction codes and infotypes (in HR), end users will be using. These transaction codes and infotypes are grouped into Security Roles. There are two groups of security roles.

- The first are Simple Security roles. The simple security roles are functions and are a grouping of transactions and infotypes. When building the simple security roles, we build simple security roles that are consistent across the agencies (like HR Organizational Maintenance or Pay Maintenance). We also build simple security roles that include the differences within the agencies. But to reduce the number of simple security roles and reduce redundant security roles, the rule stands to include the similarities in a simple role and include the differences in separate roles. For example, if there are certain infotypes within HR Organizational Maintenance that only one agency will be allowed to do, then those differences would go into a separate simple role and mapped accordingly. The consistencies of HR Organizational Maintenance across the agencies would be in one role and mapped accordingly.
- Next the simple security roles are mapped to Composite Security Roles, which are tied to HR positions or jobs. This process is for the purpose of enabling the HR position or job to have access to the functions required for that job or position. Thus, the Composite Security Role will have many simple roles assigned based on the responsibilities required for that position or job.

The following picture shows the SAP Application Security Construct for mapping the transaction codes and infotypes to roles, positions, and end users.



3.2. Transaction to Role Mapping

Security Matrices are used during the design phase to help establish the security design. The Security Matrix lists the mapping of transaction codes and infotypes to simple roles. The Security Matrix helps to view the roles in an easy-to-read format and helps the SAP Security Team communicate to the functional teams the security roles being configured. The functional teams can use the security matrix to assist in adding the roles to their BPPs (business process procedures). The BPPs are used for building training and integration testing scenarios. Security is tested during integration testing and the teams use the security role listed on the BPP to test SAP security. The following shows an example of a security role matrix.

				Benefits		
		Dept 'D', Central 'C', Both 'B'		B	B	B
Transaction Code	bg = BACKGROUND (NOT ON MENU)	Transaction Description		Benefits Administration	COBRA Administration	Display Benefits
BENEFITS						
HRBEN0001		Enrollment Plans in SAP		X		
ANNUAL		Annual Enrollment				
PLAN		NC Flex Plan		U		D
PLAN		State Health Plan		U		D
PLAN		Savings Bond Plan (populate lty 0103) -- See below		U		D
PLAN		Outside of SAP - Interfaced				
PLAN		401K				
PLAN		457		D		D
PLAN		403B		D		D
PLAN		College Savings Plan		D		D
HRBEN0004		Evidence of Insurability		X		
HRBEN0014		Termination of Plan Participation		X		
HRBEN0003		Participation Monitor				X

Security Matrix being shown is only an example. The security matrix for the Beacon project is developed during Blueprint and updated throughout the Realization and Final Prep Phases.

				Benefits		
		Dept 'D', Central 'C', Both 'B'		B	B	B
Transaction Code	bg = BACKGROUND (NOT ON MENU)	Transaction Description		Benefits Administration	COBRA Administation	Display Benefits
PA Infotypes - P_ORGIN						
PA20		Display HR Master Data		X	X	X
PA30		Maintain HR Master Data		X	X	
Infotypes - P_ORGIN						
R		**READ ONLY (VALUES M, R)**				
U		**UPDATE (VALUES E,S,D,V)**				
0000		Actions	MD - Action	R	R	R
0001		Organizational Assignment	MD - Action	R	R	R
0002		Personal Data	MD - Action	U		
0003		Payroll Status	PY	R		
0005		Leave Entitlement	TK			
0006		Addresses	MD - Action	R		
0007		Planned Working Time	MD - Action/TK	R		R
0008		Basic Pay	MD - Action			

Also, included in the security matrix are the infotypes mapped to each role. This will indicate the appropriate access assigned to the role (e.g. read, write, update, delete, etc.).

3.3. Role to Position Mapping

Once the simple security roles have been defined, the SAP Security Team will work with the Change team for "Simple Role to Position to User Mapping". This process helps to define the users required for training. It also achieves our understanding of what access is required for each user. Since we will be using Position Based Security, it is necessary to gain an understanding of users to roles and then map those roles to the user's HR position. The concept of Position Based Security is automating the access for the user based on the HR position to which the employee is assigned. The result is that the security roles are mapped to HR positions, which employees will inherent, and thus employees will automatically have access to SAP with the access required to SAP based on their HR position.

4. SAP SECURITY ORGANIZATION HIERARCHY

SAP Security Organization Hierarchy is the ability to secure by different organizational levels. For the State of NC, it will be ensuring the ability to secure the different agencies appropriately. In the current legacy system, HR and Payroll are on separate systems. Thus, HR does not have access to Payroll. Payroll does have view access to HR, but not update. Additionally, in the current legacy system, HR and Payroll are restricted to only view and update data for their own organization (i.e., secured by department, division, and section). By using SAP, Payroll and HR are integrated.

Without properly implementing SAP Security Organization Hierarchy, it could open the access for agencies to update or display each other's data that may not be intended.

4.1. SAP Security Organization Hierarchy Requirements

To ensure the SAP Security Team implements agency restrictions that should be in place, the SAP Security Team will work with the functional teams to obtain the SAP Security Organization Hierarchy Requirements. The requirements needed include the following:

- Gain an understanding of which agencies should and should not see or update another agency's data. SAP has provided a means for the SAP Security Team to secure agency restrictions from an update or a display perspective.
    - For example, access to display an agency's data can be granted without granting update to the agency's data, or no access to another agency's data from a display or update perspective can be achieved.
- Gain an understanding of these organization hierarchy restrictions based on the SAP transactions or functions. SAP has provided a means to secure by functions.
    - For example, security can be established to grant agencies to display each others cost centers, but not HR master data.
    - Another example, access to infotype 0001 (which is organizational assignment) can be granted to all agencies, but access to infotype 0008 (salary) can be restricted by agency.
- Gain an understanding of organization hierarchy restrictions within an agency. Depending on the module being implemented and what is configured, SAP has provided a means to secure within an agency.
    - For example, understanding if there is a need to restrict within Department of Correction and if there are restrictions, understand what they are.

The means SAP has given to secure by SAP Organization Hierarchy Security is by security authorization objects. The different security authorizations provide the ability to secure different areas differently based on the security requirements. The requirements obtained and implemented will be documented in a document called "SAP Security Organization Hierarchy". This document is completed during Blueprint and continues to be updated throughout the Realization and Final Prep Phases.

4.2. Common Organizational Areas for Securing SAP Hierarchies

The following include the most common Organizational Areas used to secure by SAP Security Organization Hierarchy for HR, FI, CO, and FM:

- Human Resources – (PA/Benefits/Payroll)
    - Personnel Area
    - Personnel Group
    - Personnel Sub Group
    - Organization Key (field available to include any of the following and thus able to be secured on by Cost Center, Organization Unit, Personnel Sub-Area)
    - Admin Groups (Payroll Admin, Time Admin, Personnel Admin)
    - Payroll Area

- Human Resources – Organizational Management (OM)
  - Organization Unit
- Human Resources – Time Management
  - Org Structure or
  - Cost Center
  - Data Entry Profile
- Human Resources – Training and Events
  - Course Group
- Finance
  - Company Code
  - Business Area
  - Funds Center
  - Vendor Account & Authorization Group
- Controlling
  - Controlling Area
  - Cost Center
  - Cost Element
  - Profit Center
- Funds Management
  - Funds Area
  - Funds Center
  - Funds

4.3. Using SAP Derived Roles for SAP Security Organization Hierarchy

When securing by SAP Security Organization Hierarchy, "Derived Roles" will be used within the Profile Generator Tool. "Derived Roles" allow the transaction codes and infotypes within the role to be same for all agencies, while restricting each agency by the SAP Security Organization Hierarchy that is defined. Using Derived Roles will simplify security administration. Instead of having to change an authorization or add a transaction code to each agency role, only one role has to be updated and then each agency will inherit the change, but yet keep the organization hierarchy restriction. More details on how to use Derived Roles is explained in the SAP Security Policies and Procedures and in SAP's Security Guide, Authorizations Made Easy.

5. TECHNICAL SECURITY GUIDELINES

There are certain transaction codes within the SAP system that should not be granted to end users in the Production System(s). These transactions allow changes to be made in the production system without going though the established change process. Allowing these transactions to be run in production can cause the SAP system to get out of sync with the development and quality systems.

5.1. Program and Report Security

Custom transaction codes are created to run custom ABAP/4 reports and programs. To ensure users are accessing transactions that have been tested and approved for a user to have access to run, access to SE38 and SA38 are not allowed. SE38/SA38 would allow any custom program to be run from a single transaction with only one set of authorization controls. The following guidelines are being used in relation to Program Security:

- Production end users will not be assigned access to SE38 or SA38.
- All programs (custom and standard SAP) will be executed by assigning a transaction code to the program, and users are granted access to the transaction code by having the security role assigned to the transaction code. Thus users do not require access to SE38 or SA38.
- Standard SAP programs and reports check security organization hierarchy restrictions. However, custom programs or custom reports do not check security organization hierarchy by default. Security organization hierarchy can be checked in custom programs by adding Authority-Check statements into the program. The functional teams are responsible for determining if security organization hierarchy requirements are needed for any custom program or custom report. Once it is determined what security should be checked, the functional teams will communicate to the Security Team what is required (i.e., need program to check personnel area). Then the Security Team will inform the ABAP programmer which security authorization object to check in the program based on requirements. If standard security authorizations are not available, the Security Team will determine if custom authorization objects are required and create if needed. Policies and procedures will be documented on creating custom authorization objects in the SAP Security Policies and Procedures. Security for custom programs is addressed in the Development Standards document.
- SE38/SA38 may be granted for the project team members for go-live/cutover activities only. The Basis and SAP Security Teams is the only exception where this team will be allowed to have SE38 after go-live. Project Team Members and Support Staff will not use SE38/SA38 after cutover (instead tools like code comparison between development and production can be used to check if code is in sync).

5.2. Table Security

The ability to view or update a table should be restricted appropriately. Table Security is highly controlled because when viewing or updating a table, SAP Security Organization Hierarchy is NOT checked. Thus, if a user has access to the table, the user has the ability to see all the data in the table. For example, if a user has access to table PA0008, then the user would be able to see all salaries for all agencies with no security organization hierarchy being checked.

SAP intended users to access data via functional transaction codes or report transaction codes instead of accessing tables directly. Transaction codes query the data in the SAP tables in a manner to cause less stress on the system. Also, transaction codes check security authorizations that can allow securing by Security Organization Hierarchy. However, in certain situations, tables may be required to be viewed or updated by a

certain group of end users. If a table is required to be viewed or updated, the content of the data in the table should be considered.

To control the risks associated with tables, the following guidelines are being used related to Table Security:

- Transaction codes SE16, SE16n, SE17, SM30, and SM31 will not be given to the general end user population. Project team members and Support Groups will be granted access to these transaction codes since they require checking tables that were transported and since they need to see all agencies data.
- In the situation where a table is required to be granted to an end user, a custom transaction code will be created that gives access to only the one table that is required. The custom transaction code will be mapped to a role, which is mapped to the user's position. It is uncommon that end users will need very many tables. So for any table that is required to be given to an end user, a separate transaction code will be created for each table. Also, some tables already have a standard SAP transaction code assigned to update the one table. For example, transaction code S_ALR_87003642 or OB52 is used to open and close FI periods.
- SAP tables are grouped into authorization groups, which are logical grouping of tables based on the functions the tables perform. Custom Tables by default are not assigned to an authorization group. The SAP Security Team will assign all custom tables to an authorization group and group based on functional group (i.e., payroll, time, finance, etc.).

5.3. Spool Security

SAP print spool is where print jobs are sent if a printer accidentally jams or if a user intentionally sets the print job to not print immediately. If the print job does not have the "Print Immediately" button set, then the print job will not print to the printer, but rather will go to the print spool. Also, sometimes users want the print job to go to the print spool so they can view the print job before printing out a large job.

The risk associated with print spools is a user could see another user's print job and the data in the print job could be sensitive. To control this risk the following guidelines are being used related to Spool Security:

- All users will be allowed to see their own print spool. However, access to see other users' print spool will not be allowed. Because of how payroll jobs run, payroll users are sometimes an exception and need to see other spools. Project team members and SAP Support also normally require access to see all spools. If any group of users is an exception and requires access to see all spools, it will be approved by management during final prep.
- During the implementation, if it is discussed that users need to see other users spool, then the following process will be implemented. Batch IDs can be setup and access to the batch IDs print spool can be assigned to a role and granted access. Normally, if this is required, then batch IDs for each functional area and each agency would need to be setup to restrict agencies to see only the print job based on the agency and area (i.e., HR vs. non-HR). This process will be implemented, if required.

5.4. Printer Security

Printers in SAP are defined by the Basis Team. Users normally use the LOCL printer in SAP, which points to and prints any job to their Windows Default Printer. However, sometimes certain printers are set that need to be restricted to only certain users to access. These printers are normally for printing AP and Payroll checks.

Printers are secured by using Authorization Groups on the printers. Authorization groups allow printers to be grouped. Security is then built by granting access to the printer authorization group.

During the implementation, special printers will be defined. If a printer is defined to be restricted, then these guidelines will be used to restrict printer access. If additional grouping of printers are required, then authorization groups will be added and assigned based on requirements.

- GENERAL – This authorization group will be used for General purpose printer. ALL users will have access to any printer with the authorization group GENERAL.
- SECUREHR – This authorization group will be used for check printers. Only users requiring access to the check printers will be allowed access to any printer with the authorization group SECUREHR.

5.5. Default SAP User IDs

The special SAP user IDs that can be used to log directly into (dialog) SAP include: SAP* and DDIC. These user IDs are users that are defined when SAP is loaded. These passwords must be changed immediately, since the default passwords are well known to the public. The new password should be held in a protected environment with only authorized individuals knowing the password.

The following guidelines are used to ensure the default SAP User IDs are secure properly:

- **SAP*** user master record will be locked and not able to be logged onto. The roles and profiles assigned to SAP* user ID will be removed, rendering it unable to execute any SAP transactions. Additionally, the SAP* ID will not be deleted in any system or client. If SAP* user ID is deleted, SAP automatically regenerates SAP* and resets the password to its default. At this point, the SAP* ID is given unlimited access as it is not subject to authorization checks. If SAP* is ever accidentally deleted, the user ID will be recreated, locked and all access removed. In place of SAP*, another super ID (i.e., SAPADMIN) may be created to use for loading patches, OSS notes, etc. SAP* user ID, if used in production, should only be used in case of extreme emergency where no other user can access the system.
- **DDIC** user ID needs to be used to load patches, OSS notes, or other system support tasks. DDIC does require being active; however the password must be changed and stored in a protected environment. The password should be a strong password that is difficult to guess.
- Ownership of Default User IDs
    - In the development and QA systems/clients, the Basis Team will reset the passwords and store the passwords for DDIC and the id that replaces SAP*. In the production systems, the SAP Security Team will be responsible for resetting the passwords and storing the passwords.
    - In production, the SAP Security Team will grant access to these user ID's on a temporary as-needed basis only. Access will be granted only after receiving an approval from the State Technical Leads. The SAP Security Team will grant access for only 24 hours in the system and will immediately change the password after receiving notification that use of the super user ID has been completed. Additionally, the reason for needing to use SAP* or DDIC will be documented.

5.6. Client 000, 001, 066

Client 000 is supplied with every installation and serves as a default maintenance client. Client 001 is another SAP client and is a reference client. Additionally, client 066 is the SAP EarlyWatch client that is also delivered

with SAP. The EarlyWatch client is used for log in by SAP and does not have any State of NC master data. The Basis Team is the only group that uses and will have access to clients 000, 001 and 066 clients.

5.7. SAP_ALL

SAP_ALL is a profile that is delivered with SAP which allows access to execute all transactions within the system. In non-Production systems, SAP_ALL will be assigned to Basis and Security Team members to troubleshoot technical and security issues. In Production, a 'near' SAP_ALL will be given to selected members of the Basis Team for cutover and go-live activities. After cutover, a Basis Administrator role will be used for Basis Team members. Additionally, at times, SAP_ALL may be used by the SAP Security Team to verify whether or not a unique problem is security related or a SAP internal problem. The SAP Security Team may troubleshoot security problems at times by granting an end user temporary access to SAP_ALL and tracing the user while they have this access. If the user still has the problem with SAP_ALL, then the SAP Security Team is certain the issue is not security related. Lastly, SAP_ALL may need to be granted to the Basis Team or SAP for troubleshooting.

6. USER MENU

There are two types type of menus within SAP, User Menus and SAP Menus. SAP Menus show all transactions available to be executed in the system. However, the users would only be able to execute the transactions which have been assigned to them within a security role. User Menus are built by Security within profile generator. User Menus show only the transactions the user has access to execute. The User Menus being built will follow the SAP Menu path, which is being trained. User Menus simplify the user appearance of SAP, since only the transactions their security allows them to use are visible.

7. USER ID

7.1. User ID Naming Convention

SAP User IDs in ERP2005 and BI can be up to 12 characters in length. Portal User id length is based on what has been set in LDAP. Portal and LDAP User IDs are allowed to be up to 200 characters. However, if using an ABAP engine as the user data source, the User id can only be up to 12 characters in length. There are no restrictions on the characters of the User id as long as it is within the length allowed.

A couple of options for naming the user id are being considered. The State of NC is close to a resolution. The choices being considered include the following:

- SAP user ID may be named the same as the NCID. If decided, then NCID will need to change their requirements of the length to be limited to 12 characters.
    - Pros include: no mapping table to NCID from SAP is required
    - Cons include: SAP user id will need to come from an outside SAP source and consideration of non-employees not entered into SAP HR.
- SAP user ID may be something other than the NCID (i.e., the employee's personnel number)
    - Pros include: less effort to automate user id creation
    - Cons include: consideration of non-employees not entered into SAP HR

Authentication of user access is defined in detail in the User Access Strategy. Please refer to the User Access Strategy document.

Additionally, end users should only require one user ID. If there is a situation related to segregation of duties conflicts, then the security administrator will work with the data owner to decide on a resolution, but this will not allow for using multiple user IDs.

7.2. User ID Automation Strategy

The Security Team will write a spec to determine if a program can be written to automate the user ID creation process and creation of infotype 0105 subtype 0001. Additionally, the Security Team will be writing a spec to determine if a program can be written to automate the creation of the Portal user ID from ERP2005 user ID creation. Usage of Central User Administration (CUA) is being considered to automate the creation of the BI user ID for production from ERP2005. If CUA is not used, then a program spec will also be written for the automation of creating the BI user ID. These programs would ensure the user IDs in ERP2005, BI and Portal production systems have the same user ID in all environments. Additionally, these programs would result in a timely user creation process.

The Security Team would also like to automate the assignment of security roles in the portal. This program would be based on the naming conventions of the SAP Security roles. A trigger of ESS and MSS roles being assigned in SAP ERP2005 would initiate the user assignment in the Portal. If requirements show there are multiple ESS and MSS ERP2005 roles required, then a mapping table may be needed to identify which ERP2005 roles get mapped to the portal roles.

7.3. Deactivating User IDs in SAP

User IDs will not be deleted in SAP. Instead when a user ID is no longer needed, the following will be completed:

- Lock User ID
- In the Valid To Field in the user master record (user id), a date from when the user access would be denied would be set. If the user attempts to login, the system will not allow the user to log in and a message, “User not in validity date. Please inform administrator.” will display. This Valid To date being in the past is also how SAP monitors User Licenses and thus it is very important to set a user to an invalid date when deactivating the user ID.

Put User ID in User Group → ZZNO _LONGER. This will help to know the user ID is not active and useful for reporting analysis.

7.4. Transferred or Terminated Employee Process

A program will be written to identify when employees have transferred or terminated from the State of NC. The SAP Security Team will use this information to ensure employees that have left the State are deactivated in SAP. Additionally, NCID will receive this information to synchronize all other non-SAP systems with this information.

8. CENTRAL USER ADMINISTRATION

Central User Administration (CUA) is a tool that is available to administer security. With CUA you can reduce the security administration efforts to maintain users. CUA allows you to maintain the users centrally in one system. The information is then automatically distributed to the dependent systems. So when creating new users, the user would only have to be created once instead of being created in each client. CUA will be evaluated based on using functionality of administering users from a central instance with users only having one user ID (users must have same user ID in all SAP systems).

Pros for using CUA

- Easier for security administration
- Easier on security maintenance
- Keeping User IDs consistent for users across all systems/clients.

Cons for using CUA

- More work for the Basis Team
- Learning curve for Basis and Security Teams
- Troubleshooting and time will be required on Security Administrators and Basis Administrators to get CUA to work correctly
- If client copies or refreshes are done, user IDs are not copied. If it is a requirement to copy the user IDs, then disabling CUA is required until the client copy/refresh is done.

Based on the benefits of CUA and the fact the State has and will have many sandbox, development and QAS clients, the Security Team will evaluate using CUA. By using the tool, the Security Team will be able to decide if the benefits outweigh the cons.

A decision will be made after using CUA to determine if CUA should be used for the production systems. If CUA is used for production, then CUA will be setup separately in production from the non-production systems/clients. Since production end users are a different group of users from non-production end users, it makes sense to have CUA setup separately. Also, it is better to setup separately since non-production may be on different maintenance schedules.

9. PASSWORD ADMINISTRATION

SAP has some standard default password requirements, which are not part of the SAP system settings, but are standard for all SAP systems. The following are default requirements in ERP2005 and BI that can not be changed:

- Password length can be up to 40 characters in length
- First character may not be ! or ?
- First 3 characters in a password may not appear in the same sequence in the user ID (for example, user id CWELLS would not be able to use WELCOME123 as their password because WEL is in the user id)
- First 3 characters in a password may not be identical (for example, aaa, bbb, ccc)
- Space character not allowed within first 3 characters
- Password may not be PASS or SAP* (* meaning any string of character(s))
- Any character is allowed
- Passwords are case sensitive
- A user can change their password only once a day

- Passwords may not be the same as any of the previous five passwords used

10. SAP SYSTEM SETTINGS

SAP System settings will be established based on existing State of NC standards. The strategy includes for the SAP Security Team to work with the State of NC Security Group to ensure the SAP settings are set according to company standards. The SAP Security Policies and Procedures document will include what settings have been set based on decisions made by the State. The login related system settings are just applicable to a few maintenance users that will have direct access to the SAP systems. All other users will have their password deactivated in the SAP system and will be authenticated by the NCID integration. The following include the settings to be reviewed:

			RECOMMENDED VALUES		
SAP System Profile Parameter	**Description**	**SAP Supplied Default Value**	**SBX/ DEV Systems**	**QAS/ TRG Systems**	**Prod Systems**
Login/fails_to_session_end	Number of invalid logon attempts allowed before the SAP GUI is disconnected.	3	3	3	3
Login/fails_to_user_lock	Number of invalid logon attempts within a day before the user id is automatically locked by the system.	12	12	12	6
Login/failed_user_auto_unlock	Disable system function for automatic unlock of users at midnight. 1 means requires administrator to unlock.	1 = Do Not unlock at midnight	1 = Do Not unlock at midnight	1 = Do Not unlock at midnight	1 = Do Not unlock at midnight
Login/min_password_digits	Defines the minimum number of digits (0-9) in passwords	0	1	1	1
Login/min_password_letters	Defines the minimum number of letters (a-z) in passwords	0	1	1	1
Login/min_password_lng	Minimum password length for user password	3	8	8	8
Login/password_expiration_time	Number of days after which a password must be changed	0	0	45	45
Rdisp/gui_auto_logout	Number of seconds that must elapse before a user is automatically logged off due to inactivity.	0	1 Hour	4 Hour	1 Hour

11. SINGLE SIGN-ON

Single sign-on capability will be used for user authentication in the SAP systems. This allows the authentication to happen at the front end systems. Once authenticated, access to other SAP systems will be granted via SAP logon tickets, therefore passwords will not be maintained in each SAP system. The mechanism used is described in the User Access Strategy document. This document diagrams the user authentication process, including single sign-on. The password restrictions outlined in Section 9, would not apply in a single sign on implementation where user authentication is occurring in a separate system. For contingency reasons, there will be a limited amount of ID's where the passwords will be maintained in SAP to allow for system maintenance access to the application servers in case of a failure of NCID.

12. SEGREGATION OF DUTIES STRATEGY

A Segregation of Duties (SOD) analysis will be completed when building the SAP Security Roles. To understand Segregation of Duty conflicts, the SAP Security Team will work with the functional teams to design an SOD matrix. Since the Beacon project is working on the HR module, less SOD conflicts will exist. FI and Supply Chain modules are expected to have more SOD conflicts. When those modules are implemented, an analysis will be made to determine if additional tools will be required. At this time, a review will be completed and a matrix created. The following includes an example of an SOD matrix for Accounts Payable. Note: If the spreadsheet will include when mitigating controls are in place and thus mitigates the conflicts. A similar matrix will be created for HR and will include conflicts and mitigating controls specific for HR and the Beacon project. AP was shown as an example since these are most widely known and easily understood.

Segregation Of Duties Conflicts By Transaction - ACCOUNTS PAYABLE			Vendor Master Data Maintainer - AP	AP Invoice Processor	AP Payment Processor	Mitigated
Transaction	**Transaction Text**	**Role**				
Conflict #1 Allowed because of Mitigating Control						
F110	Parameters for Automatic Payment	ZFI-PROC_VENDOR_PAYMENTS-MSTR			Allowed	Create Vendor with Processing AP Payments will be allowed because mitigating control.
FK01	Create Vendor (Accounting)	ZFI-MTN_VENDOR_MASTER-AP	Allowed			Mitigating control includes Vendor Create/Change Report will be reviewed by supervisor to ensure all vendor creations/changes are appropriate.
Conflict #2 Allowed because of Mitigating Control						
F110	Parameters for Automatic Payment	ZFI-PROC_VENDOR_PAYMENTS-MSTR			Allowed	Change Vendor with Processing AP Payments will be allowed because mitigating control.
FK02	Change Vendor (Accounting)	ZFI-MTN_VENDOR_MASTER-AP	Allowed			Mitigating control includes Vendor Create/Change Report will be reviewed by supervisor to ensure all vendor creations/changes are appropriate.
Conflict #3 Not Allowed - If User has both Security Roles, then ISSUE						
FCH7	Reprint Check	ZFI-PROC_VENDOR_PAYMENTS-MSTR			X	
MIRO	Enter Invoice	ZFI-PROC_AP_DOCUMENTS-MSTR		X		
Conflict #4 Not Allowed - If User has both Security Roles, then ISSUE						
F110	Parameters for Automatic Payment	ZFI-PROC_VENDOR_PAYMENTS-MSTR			X	
MIRO	Enter Invoice	ZFI-PROC_AP_DOCUMENTS-MSTR		X		

13. SAP USER GROUPS

SAP User Groups are placed on user master records for each user ID. User groups are used to more efficiently report on users (i.e., identify HR from FI, portal from back office, etc). Also, user groups are used to secure by user group. For example, if a helpdesk should be able to reset passwords for end users, then user groups can be used to restrict the helpdesk on which users they can reset passwords. So access can be restricted where the helpdesk can't reset a background id password or Basis/SAP Security Team's password. User Group definitions will be defined closer to go-live and will be documented in the SAP Security Policies and Procedures document.

14. SECURITY AUDIT LOGGING AND REPORTING

Any update activities done on SAP data is tracked by the user ID that made the change. No activation of logs is required for SAP to track these changes. Additional to the normal tracking done is SAP Audit Logs. These SAP Audit Logs can be activated to track certain activities. Since these logs take disk space on the server, it must be considered what type of audit logging should be activated. The logs that should be activated should be based on procedures for reviewing the information captured in the logs. The SAP Security Team will review during final prep phase which audit logs would be reviewed periodically. The SAP Security Team will work with the Basis Team to activate the SAP Audit Logs in the production system. A process will be setup to review the audit logs periodically by the SAP Security Team. These procedures will be documented in the SAP Security Policies and Procedures document.

SAP also provides security reporting. The reports available allow reporting on user logon activity and user access. Procedures will be developed to run certain security reporting periodically. These procedures will be documented in the SAP Security Policies and Procedures document.

15. CHANGE CONTROL FOR SECURITY

The Security Team will follow the same change control procedures that are setup for the SAP project. The Basis Team has diagramed the landscape environment. All security configurations (i.e., security roles, table authorization groups, etc) are created in a development environment and transported to QAS, Training and Production. This process ensures the security roles are transported and are kept in sync between development, QAS, Training and Production. The change control process exists for BI, ERP2005 and Portal.

At go-live, it may be necessary for the Security Team to be granted temporary approval to update security roles directly in the production environment. The temporary amount of time is dependent on how long the stabilization period exists for the project or for the Security Team. The reason for this access to be granted is to ensure quick response on fixing security issues. At go-live, more issues may arise and it is necessary to ensure a minimum amount of disruption to our end users. Although security will be tested extensively, not every single function within a transaction is possible to test, and thus an issue may arise at go-live that would not have come up during testing. Therefore, the Security Team may be granted access in the production environment to fix a security role, ensuring the least amount of disruption to our end users. The Security Team will still update the security role in development, and transport the changes to ensure all systems/clients are in sync with production.

The Security Team will discuss if this will be allowed for go-live and the time period allowed. This discussion normally occurs close to go-live when project teams' access for go-live/stabilization period is discussed.

16. SAP ENVIRONMENTS

A brief explanation of the SAP environments is contained below. Security is constructed based on the access requirements for each environment.

16.1. Sandbox Systems

The Sandbox system exists to allow the technical team to perform tests on new SAP patches and upgrades, OS patches or upgrades, and database patches or upgrades without affecting the project team. Only after changes are tested in the sandbox are they applied to the other SAP environments (including BI and ERP2005 systems). Neither the data nor the configuration in this environment is carried forward into other environments.

16.2. Development Systems – ERP2005 Configuration Client

All configuration is completed in the configuration environment and transported to the integration and production environments. Configuration clients are always in the development system.

Update configuration access is restricted to the functional teams. Team members include Project team and support team members that configure the system. In addition, Basis and Security Teams have access to support the environment.

16.3. Development Systems – ERP2005 ABAP development Client

Programmers create and change custom ABAP code in the ABAP environment. ABAP code is client independent and when a program is created in one client, it resides in all clients on that system. Programs are developed in the ABAP client and transported to the integration and production environments. ABAP clients are always in the development system.

Access to the development client is restricted to the programmers. Also, Basis and Security Teams have access to support the environment.

16.4. Development Systems – ERP2005 Security Client

It is under consideration for Security to have their own client to configure security roles. No decision has been made whether this consideration will be certain. If a security client is created, then access to the client will be restricted to the Security and Basis Teams only. The technical team leads will make a decision if a security client will be created in the ERP2005 system. The pros and cons of having a security client are listed:

Pros to having own client

- Since Security has different requirements on transports, the transport path is easier to distinguish if Security had its own client.
- Better place to setup CUA
- Security roles are client dependent and can limit their existence to their security client.

Cons to having own client

- More work for Basis Team (minimal)
- More space on server required
- More work on Security Team (minimal)

16.5. Development Systems – Business Intelligence (BI)

The BI development system only has one client. All configuration and programs are developed in this environment and transported to the BI integration and BI production environments.

BI team members have access in this system. Certain functional and programmer team members may require access in BI also. If determined the functional and programmer teams need access, based on the data, certain security roles will be created to restrict appropriately.

16.6. Quality Assurance and Testing Systems - Integration Testing Client

Configuration, programs and security roles are transported to the Testing client (Quality Assurance System) via the Transport Management System. The source for all transports within the system landscape is always the development environment. In general, no configuration is allowed in this client (except some rare cases, where system specific settings need to be done). Additionally, programmers are not allowed to change programs in QAS. All program changes will be required to be changed in development and transported via the change control process. Programmers will have display to debug in QAS, but they will not be allowed to change values. Integration testing is always performed in the QA system.

Integration testing of functionality and security is completed by the functional teams and testers. Testing security is completed by having testers use test IDs that would function like production roles/end users.

16.7. Training Client(s)

A training environment (separate systems) will be established to provide an area for training. Instructors who are creating training materials will be granted access to the training system. Project team members and support teams are also granted access, to complete any manual configuration and to load master data, if required. Training IDs for trainees are created and assigned access to perform all SAP transactions. Additionally, instructors are allowed access to reset passwords for trainees.

16.8. Production Systems

The Production environments are built via transports from the configuration of the development clients. Transports are sent to production after testing in the Quality environment. No configuration is allowed in this environment (except some rare cases, where system specific settings need to be done). Additionally, programmers are not allowed to change programs in PRD. All program changes will be required to be changed in development and transported via the change control process. Programmers will have display to debug in PRD, but not allowed to change values.

17. SENSITIVE DATA

The SAP Security Team will work with the appropriate parties (i.e., functional team, OSC, OSP) to determine what data is considered sensitive for the State. Also, general statutes will be reviewed to determine if the statutes can add information on sensitive data. Sensitive data will be carefully evaluated and access will be restricted appropriately. Non-production systems that are less secured may have the requirement for the data to be scrambled.

18. SECURITY TESTING

Security is tested during integration testing in the QAS environment. The testing team will consist of functional team members, including subject matter experts and project team members. Users will complete integration testing by using test user IDs. Test IDs will be setup to equal each security role. Testing with these test user ID's ensures that the access is restricted appropriately for end users after go-live. In order to allow security to be tested appropriately while not hindering the testers from completing their functional test scripts in an efficient manner, the Security Team will be adjusting immediately any security related challenges that might come up during testing. Also note, ESS and MSS test IDs will be setup to work like an ESS and MSS user in production. The security role assigned will be restricted to ESS for the ESS test user and MSS for the MSS test user. This will ensure a user with only access to ESS or MSS will have the correct access after go-live. Additionally, users will be testing via the same authentication process as users in the production environment will have after go-live. Thus, the authentication method is tested. To understand the authentication process being used, please refer to the User Access Strategy document.

After go-live, security is also tested in the QAS environment. Once the security works correctly in the QAS system, changes to security are moved to production.

19. SAP SECURITY REQUEST PROCESS

A SAP security request process will be established. The process will include a security request form. Data owners will be established and these data owners must approve access before access is granted.

19.1. Production

Position based security will be used in the production environment. When employees are hired or change jobs, security will be automatically created or changed based on the job. This is achieved by assigning roles to positions. The Security Team will gain an understanding of which security roles can't be mapped to positions when the Change Team completes the Security Role to Position mapping. The current plan is to map all roles to positions via position based security except ESS roles. The ESS and General role that all users are intended to receive will be added during user creation and linked directly to the user ID.

A security request form will still be required for certain situations in production. Examples of these situations are when the user is not an employee and is not in SAP HR as a non-employee or when an employee may require a former job's security access temporarily or if a user requires one role removed and another role added for segregation of duty conflict issues. Thus, a security request form will be created to request and approve access since position based security cannot achieve these examples. In the situation where position based security grants access to the user based on the user the position holds, no request form will be required. But rather, as part of go-live, the approval will be completed by the data owners to approve the security role assignment based on the HR positions. The process will be documented within the SAP Security Policies and Procedures.

19.2. Sandbox/Development/QAS

Development access is not secured by transaction code, but rather by restricting the authorization objects. By restricting the authorization objects, access is restricted by functional areas (HR versus non-HR) and by configuration versus programming, etc.

All requests for access to the development and QA systems will be approved before access is granted. A Development/QA request form has been created to request access. See Appendix B for a copy of the SAP Security Request form used for Dev/QA. The following process will be used for requesting and approving access in the development/QA systems:

1. During the On-Boarding Process, the PMO will initiate the SAP security request for user access to development and QA.
2. The PMO will obtain the approval from the data owner, which are the State Team Leads.
3. Once the approval is obtained, the PMO will send an email to BEACON.SEC@ncosc.net with the approved security request form attached.

The SAP Security Team will create the user in the appropriate SAP systems and email the user upon completion.

20. SECURITY ROLE NAMING CONVENTION

Well-designed and organized naming conventions provide much needed information and documentation for the Security Administrator. Consistent compliance with the naming convention helps to make access assignment more efficient and orderly, as well as simplifying maintenance.

20.1. SAP ERP2005, BI, Solution Manager

For ERP2005 and BI, SAP uses a standard naming convention for its own security roles and has reserved name ranges for customer security roles that are created. SAP has reserved that the first character of a custom security role, authorization, profile, or authorization object, start with a “Y” or “Z”. In addition, an underscore “_” is not recommended by SAP to be used in the second character position. Following the SAP recommended naming conventions for custom objects ensures that customized objects are independent of the SAP supplied objects and will not be overwritten during the import of a new SAP release/upgrade.

Thirty characters are available to name the technical Simple and Composite role name. Ten characters are available for the technical profile name. For each simple security role, a profile must be assigned.

The following are the naming conventions for production versus sandbox/development/QAS security roles.

20.1.1. Sandbox/Development/QAS

To distinguish Sandbox/DEV/QAS roles from Production roles, the naming convention is different.

- Simple Security Roles for DEV/QA will follow this naming convention:
  - Example = Z:F_ALL_HR (Functional Update HR)

1st	Z
2nd	: (colon) – used as a separator
3rd-10th	Description
11th-30th	Not used in development roles

- Security Profiles associated with Simple Security Roles for SBX/DEV/QAS will follow this naming convention:
  - Profile associated with Simple Security Roles for SBX/DEV/QAS will be named the same as the Simple Security Role

- Composite Security Roles for SBX/DEV/QAS will follow this naming convention:
  - Example = YERP-DV_CONFIGURATOR_HR (HR Configurator in Dev System)

1st	Y
2nd-4th	System ERP, BIW, SOL
5th	Dash - used as a separator
6 th-30th	Description

20.1.2. Production

Production Security Roles will follow this naming convention for ERP2005, BI and Solution Manager:

- Simple Security Roles for Production:
  - Example = ZHR-MTN_HR_DATA-MSTR (Maintain HR Master Data - Master)

1st	Z
2nd-3rd	Sub Module - HR, PY, TM, FI, ESS, MSS Note: for ESS and MSS, it is the 2nd -4th characters
4th	Dash - used as a separator
5th-26th	Description of Role
27th	Dash - used as a separator
28th-30th	MSTR for Master or Agency Description

- Security Profiles (associated with Simple Security Roles) for Production:
  - Example = ZHRDTAMSTR (Functional Update HR)

1st	Z
2nd-3rd	Sub Module - HR, PY, TM, FI, etc
4th-10th	Description

- Composite Security Roles for Production:
  - Example = YERP-HR_ADMINISTRATOR-MSTR (HR Administrator – Master)

1st	Y
2nd-4th	System - ERP, BIW, SOL
5th	Dash - used as a separator
6th-7th	Sub Module - HR, PY, TM, FI, etc
8th	Underscore - used as a separator
9th-26th	Description
27th	Dash - used as a separator
28th-30th	MSTR for Master or Agency Description

20.2. SAP Portal

To understand which roles and groups to assign within SAP Portal, the following naming convention will be used.

20.2.1. Portal Roles

Portal roles will be named as follows:

1st	Y or Z
2nd – 4th	System
5th – 20th	Description

20.2.2. Portal Groups

Portal groups will be named as follows:

1st	Y or Z
2nd – 4th	System
5th – 20th	Description

APPENDIX A: SAP SECURITY TERMINOLOGY OVERVIEW

This section provides a description of the SAP authorization terms that have been used in this document. Although portions of this section have been slightly modified, most of this section comes directly from the SAP security guide, Authorizations Made Easy, published by SAP Labs Simplification Group.

Term	Definition
ABAP	Advanced Business Application Programming language. A fourth generation language designed specifically for SAP. Much of the system is written in ABAP and users are able to customize the system by modifying or writing their own ABAP programs
Activity	Activity is most common Authorization Object field – Examples: 01 – Create, 02 – Change, 03 – Display, 04 – Print, etc. SAP Table TACT contains complete Activity list of all Objects.
Authorization Group	An assignment of customized values to groups of similar information. The authorization groups are used in conjunction with authorizations associated with specific authorization objects. The field can contain an alpha-numeric value up to 4 characters/digits.
Authorization Object	An element of the authorization concept. An Authorization Object contains a group up to 10 authorization fields and relationship to check whether a user is allowed to perform a certain action. The objects are checked using AND logic to determine if the user has been permitted through authorizations, to carry out the desired action. To pass an authorization test for an object, the user must satisfy the authorization check for each field in that object.
Authorizations	An element of the authorization concept. A set of permissible values (value set) for an authorization object. The values are assigned based on the fields defined in that authorization object and the required access capabilities (i.e., a value of 03 in the activity field will assign display access and value of 11 in the company code field will assign access to company 11). Groups up to 10 authorization fields.
Basis (Netweaver)	Primary component of SAP that provides the basic capabilities of the system. These capabilities include maintaining the database, providing security, providing standard mechanisms for user dialogues, and the ability to customize and modify the system.
Central User Administration	A SAP facility that allows central control and administration of users across different SAP systems (ERP and BI) and clients. This capability also works across the different non production systems (SBX, DEV and QA).
Client	Legally and organizationally independent unit on the highest level of the ERP2005 (R/3) System, for example, a group or corporation. Technically, it is a logical subdivision of the SAP data base which allows companies and data to be entered, and utilized without any interaction with data or activities in another client within the same physical SAP data base; multiple clients can be established within one physical data base and do not interact with other clients in the same data base. At least one client must be identified in a System. Separate and unique master records and most tables.
Client Dependent	Client Dependent affects client that you are in and not all clients in an instance. Examples include most configuration, security user IDs.
Client Independent	Client Independent affects all clients in system. Examples include Programs, System Parameter Settings, and Some Tables.
Customizing & Configuration	In SAP terminology, customizing is the implementation of configurations. The configuration is completed to build the SAP system to be specific to an organization. Configuration tables are used to build the organization requirements (i.e., which

Term	Definition
	personnel areas, personnel sub-areas, etc). The Implementation Guide (IMG), is used to access the tables. Additionally, a model company (IDES), a fully integrated and pre-configured system used for training, testing and demos.
Derived Security Roles	Within Profile Generator, roles can be created that are derived from another role. When creating derived security roles, you need to have a "master security role". The derived security role will inherent the transaction codes and authorizations from the master security role. The difference in the derived security role is what is included in the Organizational Hierarchy Levels. Derived security roles provide ease in security administration to support agency restrictions.
Job	A job is a general classification of work duties, such as secretary and manager. Many employees may have the same job classification. That is, there can be 20 secretaries and eight managers. Jobs should not be confused with positions (see below).
Organizational Hierarchy Security	Organizational levels are hierarchical levels to restrict one agency from another agencies data. Examples of organizational levels are plant, personnel area, business area, etc.
Position	Positions are the individual employee placements or assignments in a company (for example, secretary of marketing or a sales manager). By creating positions and creating relationships between the positions, you identify the authority structure or chain of command at your firm. Positions should not be confused with jobs (see above).
Profile	A profile is a collection of authorizations. Profiles are attached to security roles. When the security role is added to a user id, then profile is automatically assigned to the user id.
Profile Generator	The Profile Generator (PG) supports the authorization administrator setting up the authorization concept. The tool provided by SAP is used to create and maintain security roles, profiles, and authorizations. The tool is integrated into the SAP HR module and is accessed via transaction code PFCG.
Security Role	A collection of individual transactions that are executed in performing the tasks required for a particular job function. Used by Profile Generator. Generate transaction-based Simple Roles that contain one or more Authorizations, allowing particular action(s) in the system (e.g. maintain vendors). These are usually a collection of individual activities that are routinely performed together. Composite Roles are a mechanism for grouping simple roles together. The composite roles provide an efficient method for administering user access.
Transaction	A transaction is a series of related steps required to perform a certain task.
Transaction Code	An alphanumeric code used to execute a transaction in a SAP ERP2005 (R/3) system. A sequence of four up to twenty characters represents a SAP transaction.
User Master Record	User authorization information, including assigned Security Roles, address and contact information, default date format, decimal format, default printers, default data-entry screen characteristics and user parameter data. Only users with an active user master record can log into SAP. Maximum of 12 characters (alpha or numeric) can be associated to the user master record.

APPENDIX B: SAP SANDBOX/DEV/QAS USER REQUEST FORM

BEACON HR & payroll

SAP User Access Request Form
Development/QAS Systems

Please allow 2 business days for the request to be processed. You will be notified via email once setup.

☐ Add New User ☐ Modify Existing User ☐ Delete User

Full Name **(First Name, Last Name)**:	User's Email Address:	Date:
Beacon Team/Title:	Approver Name:	Approver's Email
Temporary/Contractor ☐ Yes ☐ No	Expiration Date *(If Temp.)*: From: To:	NCID

ERP2004 Demo Systems	**Client**	☐ **Functional/ Config Team**	☐ **ABAP Developer**	☐ **Conversion Team**	☐ **BI Team**	☐ **Security/ Basis**
Approvers →		*State Func Leads*	*State Tech Leads*	*State Tech Leads*	*State Tech Leads*	*State Tech Leads*
☐E1S ERP2004 – Golden	800	Config/Func	Disp Only	Disp Only	Disp Only	SAP_ALL
☐E1S ERP2004 – Demo	100	Config/Func	Disp Only	Disp Only	Disp Only	SAP_ALL
☐P1S Portal Demo	n/a	ESS/MSS	ESS/MSS	ESS/MSS	ESS/MSS	SAP_ALL
☐B1S BI Demo	100	Func	Func	Func	Config	SAP_ALL

ERP2005 IDES Systems	**Client**	☐ **Functional/ Config Team**	☐ **ABAP Developer**	☐ **Conversion Team**	☐ **BI Team**	☐ **Security/ Basis**
Approvers →		*State Func Leads*	*State Tech Leads*	*State Tech Leads*	*State Tech Leads*	*State Tech Leads*
☐E1S ERP2005 – Golden	100	Config/Func	Disp Only	Disp Only	Func	SAP_ALL
☐E1S ERP2005 – Config	200	Config/Func	Disp Only	Disp Only	Func	SAP_ALL
☐E1S ERP2005 – ABAP	800	No access	ABAP/Func	ABAP/Func	ABAP/Func	SAP_ALL
☐P1S Portal Demo	n/a	ESS/MSS	ESS/MSS	ESS/MSS	ESS/MSS	SAP_ALL
☐B1S BI Demo	100	Func	Func	Func	Config	SAP_ALL

NOT AVAILABLE AT THIS TIME

ERP2005 Dev Systems	**Client**	☐ **Functional/ Config Team**	☐ **ABAP Developer**	☐ **Conversion Team**	☐ **BI Team**	☐ **Security/ Basis**
☐E1D – Dev Golden	100	Not Avail	Not Avail	Not Avail	Not Avail	Not Avail
☐E1D – Dev Unit Test	200	Not Avail	Not Avail	Not Avail	Not Avail	Not Avail
☐E1D – Dev ABAP	300	Not Avail	Not Avail	Not Avail	Not Avail	Not Avail
☐E1D – Dev Config	800	Not Avail	Not Avail	Not Avail	Not Avail	Not Avail
☐P1D – Portal Dev	n/a	Not Avail	Not Avail	Not Avail	Not Avail	Not Avail
☐B1D – BI Dev	100	Not Avail	Not Avail	Not Avail	Not Avail	Not Avail
ERP2005 QA Systems	**Not Available**					
ERP2005 Training Systems	**Not Available**					

ADDITIONAL ROLES AVAILABLE TO BE GRANTED

Technical Access (Approvers: State Tech Leads)		**Non-Beacon User Access (Approvers: State HR Leads)**	
☐ Portal User Administration	Specify System_____	☐ All Functional HR	Specify System/Client _____
☐ Portal System Administration	Specify System_____	☐ All Functional Non-HR	Specify System/Client_____
☐ Portal Content	Specify System_____	☐ Display HR	Specify System/Client_____
		☐ Display Non-HR	Specify System/Client_____

All Beacon Team Members Completing Form will Receive:

☒ SAP Net (OSS) Access ☒ Solution Manager

Usage and Responsibility Statement: I acknowledge acceptance of the assigned user ID and recognize that the information to which I may have access is considered strictly confidential. Any software created is the property of the State of NC. The data resources of the State are to be used only for official business. I recognize that failure to comply with the policies and procedures, misuse or disclosure of my user ID, password, or data, may result in disciplinary action, up to and including termination of employment.

User	Date
Approval	Date

This form and any additional attachments should be sent through Email to: BEACON.SEC@ncosc.net